Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132
Telephone: none
Email: none

Daniel David Rigmaiden
Pro Se, Defendant

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Daniel David Rigmaiden, et al., Defendant.	No. CR08-814-PHX-DGC FIRST SUPPLEMENT TO MOTION FOR ORDER REQUIRING GOVERNMENT TO COMPLY WITH DATA DELETION REQUIREMENTS OF N.D.Cal. 08-70460-HRL/PVT, 08-70503-PVT, AND 08-70502-PVT WARRANTS

Defendant, Daniel David Rigmaiden, appearing *pro se*, respectfully submits *First Supplement To Motion For Order Requiring Government To Comply With Data Deletion Requirements Of N.D.Cal. 08-70460-HRL/PVT, 08-70503-PVT, AND 08-70502-PVT Warrants*. Based on **new legal authority**[1] that the defendant was unable to bring to the Court's attention earlier, this supplemental filing seeks to supplement prior arguments made in *Motion For Order Requiring Government To Comply With Data Deletion Requirements Of N.D.Cal. 08-70460-HRL/PVT, 08-70503-PVT, AND 08-70502-PVT Warrants* (Dkt. #847), regarding the government's failure to comply with data deletion requirements contained in the N.D.Cal. warrants.

In the defendant's motion at Dkt. #847, he requested generally that the Court order the

1. *See* United States v. Collins, Case No. 11-CR-00471-DLJ (PSG), Doc. #328 (N.D.Cal., Aug. 27, 2012), as well as Doc. #311, #313, #333, #335, #336, #348 and #360. The defendant was also only recently provided with United States v. Metter, No. 10-CR-600 (DLI), Doc. 219, p. 17 (E.D.N.Y., May 17, 2011), which was relied upon by Magistrate Judge Paul Grewal in the *Collins* order at Doc. #311.

government to comply with the terms of the relevant N.D.Cal. warrants by **(1)** deleting all forensic images containing intermingled *out-of-scope* data and other copies of data that are beyond the scope of the relevant warrants, *i.e.*, all data not copied to the CD and DVDs by IRS-CI Agent Tracy L. Daun, and **(2)** securely wiping the original physical data storage devices, seized from apartment No. 1122 and storage unit No. A-47, corresponding to the forensic images and other copied data. *See* Dkt. #847.[2] The government's response to Dkt. #847 is at Dkt. #873, p. 64-66. The defendant's reply to the government's response is at Dkt. #900, p. 13-16. The defendant assumes the reader's familiarity with those filings.

I. New legal authority applied to the matter of securely wiping the original physical data storage devices seized by the government.

After filing Dkt. #847, United States District Judge Lowell Jensen released new legal authority in the Northern District of California: United States v. Collins, Case No. 11-CR-00471-DLJ (PSG), Doc. #328 (N.D.Cal., Aug. 27, 2012).[3] In *Collins*, a defendant requested that the court order the government to return her seized Dell computer containing intermingled *out-of-scope* data not listed in a relevant search warrant. Compliance with the request made in *Collins* is similar to the government complying with the request made by the defendant in the present case, *i.e.*, to have all data securely deleted from his physical hard drives currently in the possession of the government. In both cases, the ultimate outcome is that the government is prevented from possessing *out-of-scope* data as contained on the seized physical data storage devices. In *Collins*, Judge Jensen addressed the defendant's request by first finding that "the Dell computer is a 'forfeitable instrumentality of the crime[]' [and] [g]iven that status, the government can retain the computer and the request for return is denied." *Id.*, p. 8. For the defendant in the present case, until his suppression motion is

2. Due to the government's failure to provide timely discovery, there are various factual errors made on p. 3, ln. 1-7, of Dkt. #847 that are corrected at Dkt. #867.

3. The defendant was unaware of the ruling at the time he drafted and filed Dkt. #900. The defendant is incarcerated and does not have access to up-to-date case law and his court-appointed shadow counsel uses the lower quality LoisLaw service, as opposed to LexisNexis or WestLaw, and was therefore not informed of Judge Jensen's decision.

granted,[4] he is not concerned with the government maintaining possession of the seized physical data storage devices and the defendant's request at Dkt. #847 is not a motion for return of property. In *Collins*, Judge Jensen further found that the government's right to maintain possession of the Dell computer as a "forfeitable instrumentality of the crime" also "include[s] continued possession of the out-of-scope electronic contents." *Id.*, p. 9. Judge Jensen articulated no reasoning in support of allowing the government to maintain possession of *out-of-scope* data on the forfeitable physical drive and, as explained in the paragraphs immediately below, said ruling is not fitting for the present case.

First, there is a striking difference between the search warrants at issue in the two cases. The search warrant at issue in *Collins* states: "the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant..." *Id.*, Doc. #192-1, p. 11. In contrast, the search warrants at issue in the present case mandate the government to wipe all *out-of-scope* data from seized physical data storage devices: "the government also must use reasonable efforts to destroy – **and to delete from any devices or storage media** or copies that it has retained or made - copies of any data that are outside the scope of the warrant..."[5] *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (Dkt. #566-

---

4. If the Court grants the defendant's *Motion To Suppress* (Dkt. #824), the government would be required to destroy and/or return all seized data regardless. *See* Church of Scientology v. United States, 506 U.S. 9, 13 (1992) ("Even though it is now too late to prevent, or to provide a fully satisfactory remedy for, the invasion of privacy that occurred when the IRS obtained the information on the tapes, a court does have power to effectuate a partial remedy by ordering the Government to destroy or return any and all copies it may have in its possession.").

5. Even if the Court finds the quoted clause of the "Computer Search Protocol" to be ambiguous as to which "devices or storage media" it pertains, ruling in the defendant's favor is still appropriate. In *Salceda*, being faced with a dispute regarding the government's failure to comply with an ambiguous clause in a warrant's "Computer Search Protocol," the court suppressed evidence because the tenet of *contra proferentem* requires "that ambiguities in contracts are to be construed unfavorably to the drafter." United States v. Salceda, CR 10-274 CAS, 2012 U.S. Dist. LEXIS 28211 (C.D.Cal., Feb. 27, 2012) (internal quotation marks omitted) (citing Black's Law Dictionary 328 (7th ed. 1999) and United States v. Transfiguracion, 442 F.3d 1222, 1228 (9th Cir. 2006). In the present case, the government drafted the "Computer Search Protocol" adopted by the magistrates so any ambiguities the Court may find must be resolved in the defendant's favor.

1, p. 16 (emphasis added)). IRS-CI Agent Daun has also long past copied all seized *in-scope* data to a CD and a series of DVDs.[6] The government has offered no reason as to why it needs to violate the terms of the relevant warrants and possess the original *out-of-scope* data contained on the original physical data storage devices – or even the original *in-scope* data of which the government has already copied elsewhere.

Second, unlike in *Collins*, the government in the present case does not concede that it "has no right to examine that property," *Collins*, Doc. #328, p. 9, nor has it reported that it "conducted no further examination of the property[,]" *id.*, after the initial forensic images were made.[7] The government's refusal to securely wipe the drives also raises additional privacy concerns. The government plans to initiate a forfeiture proceeding so that it can sell the seized drives to a random individual at auction. The government plans to auction off the drives in order to reduce the sought after $5,500,000.00 money judgment "by the net liquidation value at the time of sale or disposition[.]" *First Bill Of Particulars Regarding Forfeiture* (Dkt. #040, p. 2); *see also United States' Motion For Order To Continue To Maintain Custody Of Property Pursuant To 21 U.S.C. § 853(e)* (Dkt. #032). Exhibit 1 of Dkt. #040 consists of a list of items the government plans to sell including the original physical data storage devices with their appraised values. If the government sells the seized drives at auction, the very lucky bidder will gain access to a multitude of private data that neither the government nor the auction winner have any right to access. For comparison, if the government secured forfeiture and then sold one of the seized CDs containing commercially available operating system software, it would not be an invasion of privacy considering that data is neither personal nor private. However, a plan to sell personal and

---

6. *See* Dkt. #847.

7. At Dkt. #873, the government noted that "[t]he items have not been searched since they were originally mirrored and remain available to be returned upon request[,]" *id.* at 38. However, the government's response makes clear that it was referring only to the seized physical data storage devices that contain **no data** responsive to the relevant N.D.Cal. warrants. *See id*. Most of those devices were blank CDs or operating system CDs. Obviously, the defendant is not concerned with physical data storage devices that contain no data or contain commercially available software. The government's offer to return those storage devices to the defendant as some type of "token of good order" is entirely beside the point.

private data to the highest bidder is repugnant to the Constitution. *See* United States v. Metter, No. 10-CR-600 (DLI), Doc. 219, p. 17 (E.D.N.Y., May 17, 2011) ("The Court agrees with Defendant that the release to [][third-parties] of any and all seized electronic data without a predetermination of its privilege... compounds the assault on his privacy concerns."). In the alternative, if the government intends to securely wipe the drives prior to auction, there is no reason why the government should not do it now. The government has articulated no reason as to why maintaining the original *out-of-scope* data (as it now exists on the original drives) will help its case at trial. In any event, accessing, using, and even possessing the *out-of-scope* data is a Fourth Amendment violation. Magistrate Judge Paul Grewal put it best with his reasoning that "even if the law ultimately permits the forfeiture of a given device..., the law does not permit the retention of data on that device that has not been shown or even alleged to have been an 'instrumentality' of the alleged crimes." United States v. Collins, No.: 11-CR-00471-DLJ (PSG), Doc. #237, p. 12 (N.D.Cal., Mar. 16, 2012) (emphasis in original).[8][9]

II. New legal authority applied to the matter of deleting all government forensic images and copies of data created from the original seized physical data storage devices, except for the *in-scope* data seized/copied to IRS-CI Agent Daun's CD and DVDs.

Turning to the other issue raised at Dkt. #847, the *Collins* decision at Doc. #328 does not affect the defendant's request to have the government destroy all forensic images and other copies of *out-of-scope* data not seized/copied to IRS-CI Agent Daun's CD and DVDs. The request made by defendants in *Collins*, which is similar to the request made here, is still pending an ultimate outcome via a string of separate filings and an appeal to Judge Jensen:

> As for the out-of-scope electronic property contained in the mirror image copy of the computer contents that is in the possession of the government, the Court understand[s] that there is an issue as to whether the out-of-scope electronic property can be segregated and removed without causing damage to the remaining electronic contents of the mirror image. That issue is now being considered by Magistrate Judge Grewal. As to the mirror image copy of Valenzuela's computer, the government is to conduct no further

8. The order at Doc. #237 was **not** overruled by the order at Doc. #328.

9. "Nor does the law permit the retention of data outside the scope of the warrant for identification, authentication or chain-of-custody purposes." *Id*.

> forensic examination of that property unless ordered by this Court or by Judge Grewal in the matter pending before him.
>
> Collins, No.: 11-CR-00471-DLJ (PSG), Doc. #328, p. 10. *See also*, e.g., Doc. #237, #311, #313, #333, #335, #336, #348 and #360 of *Collins*.

The defendants in *Collins* request that the government "redact" *out-of-scope* data from forensic images created from seized physical data storage devices. In contrast, the defendant in the present case requests that the government's entire forensic images and other copies of data be deleted completely—other than for IRS-CI Agent Daun's CD and DVDs containing copies of *in-scope* data seized under the relevant warrants.[10] Unlike in *Collins*, the government in the present case has articulated no reason as to why it needs to maintain copies of the forensic images that contain intermingled *out-of-scope* data or even copies of forensic images that have been "redacted" to contain only *in-scope* data.[11] For example,

---

10. Prior to reading various *Collins* documents after October 22, 2012, the defendant perceived no need for the government to maintain copies of "redacted" forensic images as opposed to the copies of "extracted" *in-scope* data prepared by IRS-CI Agent Daun. If the government has a need to maintain "redacted" versions of the forensic images at issue in the present case—whether DriveCrypt encrypted virtual drives or operating system drives—the defendant has no problem with the government maintaining those "redacted" copies as long as **all** *out-of-scope* data is properly/fully "redacted" and done in a way that will prevent additional exposure to *out-of-scope* data. The ultimate goal of the defendant's motion at Dkt. #847 is to ensure that the government only possess and view the *in-scope* data copied/seized to IRS-CI Agent Daun's CD/DVDs. Furthermore, notwithstanding the outcome of the defendant's suppression filings, if the government concedes Dkt. #847 in its entirety, the defendant would also likely be willing to stipulate that certain *in-scope* software is capable of running on the seized computer system which would at least eliminate the government's probable desire to maintain possession of the operating system files IRS-CI Agent Daun failed to copy/seize while executing the relevant warrants.

11. In *Collins*, the government relied upon a declaration by Alan Lee of the "High Tech" Crimes Unit of the San Jose Police Department (Doc. #284-1) to support a claim that it is permitted to possess *out-of-scope* data because: **(1)** the prosecution needs to access *out-of-scope* Windows operating system files (apparently, agents failed to seize/bookmark operating system files as *in-scope*, even while the warrant clearly listed those files as "items" to be seized) so that *in-scope* software can be demonstrated to the jury by running said software on a clone of the defendant's operating system (Lee Dec., ¶ 11-12), **(2)** Mr. Lee lacks the skill to use a script to erase (or temporarily skip for later manual deletion) files/data that are corrupted within a forensic image and this results in a need for him to spend "thousands of hours" deleting each and every file manually (Lee Dec., ¶ 5-7, 13), **(3)** during his single 80 gigabyte drive test, Mr. Lee's carelessness resulted in his continuous accidental deletion of *in-scope* data, which caused him to repeatedly restart the manual "redaction" process (Lee Dec., ¶ 8), **(4)** nonsensical and poorly explained problems arose relating to "redacting" the Windows registry (Lee Dec., ¶ 10), and **(5)** Mr. Lee is frustrated with some search warrants not being broad enough in scope to cover the evidence he generally sees as being relevant in any given case (*i.e.*, operating system files) or, in the case of *Collins*, Mr, Lee is frustrated with agents failing to seize/bookmark the operating system files that were clearly within the scope of the warrant (Lee Dec., ¶ 15).

the government makes no claim of needing to maintain full forensic images of operating system drives in order to demonstrate software to the jury. In fact, the software at issue in the present case are "HTML Applications" that are not installed, do not use the Windows registry, and utilize only a small number of text files that are easily identified via the source code of any given "HTML Application." IRS-CI Agent Daun already copied all relevant software, source code, and the noted text files to her set of CD/DVDs containing *in-scope* data. Nevertheless, if the government wants to pursue a *Collins*-style "redaction" process, nearly all private *out-of-scope* data exists within DriveCrypt container files (*i.e.*, *.dcv files), [12] which can easily be "redacted" considering they are entirely separate from the forensic images of seized drives containing installed operating systems.[13] Notwithstanding the fact that IRS-CI Agent Daun already extracted all *in-scope* data to a CD and DVDs, if the government wants to maintain a "redacted" version of any given DriveCrypt container file (or forensic image of mounted container) it would simply need to (1) mount said DriveCrypt container file, (2) overwrite *out-of-scope* data with random data, and (3) save resulting DriveCrypt container file as "redacted" DriveCrypt container file. The reasons raised by the government in *Collins* to justify keeping private *out-of-scope* data intermingled with *in-scope* data contained on operating system drives do not even remotely apply to the images of DriveCrypt encrypted virtual drives at issue in the present case. As for forensic images of the defendant's drives containing installed operating systems, the reasons raised by the government in *Collins* are just as much invalid in that case as they are in this case[14]—

---

12. For the forensic images of drives containing installed operating systems, if the government wants to maintain "redacted" versions of those images, *see* reasoning contained in footnote No. 14, *infra*. To be clear, the defendant still wants the forensic images of drives containing operating systems securely deleted—or *out-of-scope* data "redacted" from the images if the government so chooses—considering the ultimate goal of Dkt. #847 is to have the government only possess and view *in-scope* data.

13. *Compare* Mr. Lee's declaration in *Collins*, Doc. #284-1 (indicating that all seized *in-scope* data in *Collins* was intermingled with *out-of-scope* operating system data) to IRS-CI Agent Daun's "Computer Forensic Report," *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) (indicating that nearly all seized *in-scope* data in the present case was within DriveCrypt encrypted virtual dives kept separate from the drives containing *out-of-scope* operating system data).

14. For example, for any *out-of-scope* data contained within a forensic image of a drive containing an operating system, the majority of the developed world's beginner-level

notwithstanding the fact that the government here advances **none** of the reasons it advanced in *Collins*.

This filing was drafted and prepared by the *pro se* defendant, however, he authorizes his shadow counsel, Philip Seplow, to file this filing on his behalf using the ECF system. The defendant is appearing *pro se* and has never attended law school. The defendant's filings, however inartfully pleaded, must be liberally construed and held to less stringent standards than formal pleadings drafted by lawyers. *See* Haines v. Kerner, 404 U.S. 519, 520 (1972).

LRCrim 12.2(a) requires that the undersigned include the following statement in all motions: "Excludable delay under 18 U.S.C. § 3161(h)(1)(D) will occur as a result of this motion or of an order based thereon."

---

computer users know how to select a file folder of personal family photographs and click "delete" without ruining the operations of any installed program. There is no excuse for a computer expert's failure to "redact" *out-of-scope* document data in that context. If not an exercise of incompetency, the government's use of the affidavit at Doc. #284-1 in *Collins* is an attempted duping of that court and, if need be, the defendant will seek a computer expert to ensure that said duping is not advanced in this Court. Additionally, as a general matter, if the government has a reason to maintain possession of operating system files, it can easily include those files in the list of "items" to be seized and then "bookmark" the files when conducting its forensic examination prior to expiration of the search time limit. As for "redacting" *out-of-scope* files and registry entries corresponding to *out-of-scope* installed programs, simple "file/registry watch" programs for Microsoft Windows operating systems and "extract/replay" tools for use with virtual machine players can be used to easily identify *in-scope* material. Furthermore, any number of freely available video screen-capture programs can be used to make a video of *in-scope* software running on a virtual machine clone of a seized computer and the video thereafter played for the jury post forensic image deletion. If video depositions in criminal trials are sufficient substitutions for otherwise unavailable witness testimony, they are also sufficient for computer software evidence.

Nevertheless, even the "redaction" process the government claims is too difficult in *Collins* can easily and quickly be completed as follows: (1) identify the operating system ("OS") and all installed patches on the imaged seized drive containing the OS, (2) obtain clean installation files and patches from OS provider corresponding to identified OS, (3) conduct a fresh install of the identified OS and patches on a clean government hard drive, (4) log and database the files and registry entries now contained on the government hard drive, (5) extract the equivalent of what was databased in No. 4 above from the forensic image of the seized OS drive and copy to a clean forensic image containing just those files, file properties, and registry entries, (6) play the image of the seized OS drive (*i.e.*, not the recreated slimmed down image but the original) and use any number of file/registry watch tools to identify which files and registry entries correspond to the installation/use of the *in-scope* software (*e.g.*, LOIC or HOIC in *Collins* or the HTA files in the present case), (7) extract out the files and registry entries (identified in No. 6 above) from the forensic image of the seized OS drive and copy what was extracted to the new forensic image created in No. 5 above, (8) play "redacted" image as virtual machine for the jury and run *in-scope* software demonstration. Estimated computer expert man-hours: 16.

Respectfully Submitted: November 5, 2012

PHILP SEPLOW, Shadow Counsel, on behalf of DANIEL DAVID RIGMAIDEN, Pro Se Defendant:

s/ Philip Seplow
Philip Seplow
Shadow Counsel for Defendant.

CERTIFICATE OF SERVICE

I hereby certify that on: November 5, 2012 I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Taylor W. Fox, PC
Counsel for defendant Ransom Carter
2 North Central Ave., Suite 735
Phoenix, AZ 85004

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

By: s/ Daniel Colmerauer
(Authorized agent of Philip A. Seplow, Shadow Counsel for Defendant; See ECF Proc. I(D) and II(D)(3))